

AFFIDAVIT IN SUPPORT OF COMPLAINT

I, **Bradley D. Hull**, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the Federal Bureau of Investigation, and have held this position for 7 years. I am currently assigned to one of Cincinnati Field Office's Counter-Intelligence squads. During my employment with the FBI, I have conducted and participated in several investigations involving violations of United States laws relating to espionage and the unlawful export from the United States of goods and technology restricted for national security and foreign policy reasons. I have participated in the execution of several federal search and arrest warrants in such investigations. I have had training in, and through experience I have observed, many methods used to smuggle goods and technology out of the United States and commit espionage contrary to United States law. I am responsible for investigating violations of law related to economic espionage and the theft of trade secrets (18 U.S.C. §§ 1831-1832) and export controls (Arms Export Control Act, 22 U.S.C. §2778 ("AECA") and the International Emergency Economic Powers Act, 50 U.S.C. §§1701-1707 ("IEEPA")).

2. This affidavit is intended to show only that there is sufficient probable cause for the requested complaint and does not set forth all of my knowledge about this matter. Where the contents of documents and the actions, statements, and conversations of others are reported herein, they are reported in substance and in part, except where otherwise indicated.

3. I am familiar with the facts and circumstances set forth below from my personal participation in the investigation, including my review of pertinent documents, and from my conversations with others, including other Special Agents with the FBI, and representatives of a particular U.S. company ("Victim Company A") with expertise regarding the relevant design,

testing, manufacturing data and information related to aviation technology (“Proprietary Information”). Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that **XU YANJUN (a/k/a “QU HUI”)** has attempted and conspired to obtain trade secrets in violation of 18 U.S.C. §§ 1831(a)(4) and (a)(5) (Economic Espionage) and 18 U.S.C. §§ 1832(a)(4) and (a)(5) (Theft of Trade Secrets) in the Southern District of Ohio and elsewhere.

THE DEFENDANT

4. **XU YANJUN (“XU”)** is a Deputy Division Director, Sixth Bureau of Jiangsu Province, Ministry of State Security, for the People’s Republic of China (“MSS”). MSS is the intelligence and security agency for China, and is responsible for counter-intelligence, foreign intelligence, and political security. MSS has broad powers in China to conduct espionage both domestically and abroad.

5. One of **XU**’s job duties on behalf of MSS is to obtain technical information, including trade secrets, from aviation and aerospace companies in the United States and throughout Europe. **XU** sometimes uses the aliases “Qu Hui” and “Zhang Hui” in connection with his duties. He has been known to attempt to conceal the true nature of his employment, by representing that he is associated with Jiangsu Science & Technology Promotion Association (“JAST”).

6. Beginning in at least December 2013 and continuing through the present, **XU** has worked, traveled, and communicated with individuals associated with or employed by MSS and various Chinese universities and institutions. Xu has also actively targeted specific companies in the United States and abroad that are recognized as leaders in the field of aviation and aerospace technology, design, and manufacturing (“aviation companies”). Within these aviation

companies, **XU** and other individuals, some of whom are known to law enforcement, would identify people whom they deemed potential “experts” who worked for these aviation companies, and who could be targeted and recruited to travel to China, initially under the guise or false belief that they were traveling to China merely for “an exchange” of ideas and/or to give a presentation at a university. **XU**, and others, would pay the “experts” stipends and would arrange for and pay expenses associated with their travel to China. To achieve their objective, which was to obtain specific aviation technology documents and information, **XU** and others exchanged messages regarding the types of information that they wanted to obtain, and actively discussed methods for obtaining the desired information. Furthermore, communications between **XU** and others who worked for MSS and other institutions in China reveal the methods used in order to obtain highly sensitive information from employees of the various aviation companies. As mentioned above, and as demonstrated in some of the communications detailed below, **XU** used an alias in his efforts to recruit “experts” and falsely represented his employment, all in an effort to conceal his true identity as an officer of MSS. Furthermore, **XU** and others communicated about the best way to protect and conceal the true nature of the information they were seeking from aviation companies and their employees, including the use of codes and series of letters in place of the technology being discussed and the name of the victim company targeted.

7. **XU** often communicates, travels, and exchanges information related to aviation technology with individuals at the Nanjing University of Aeronautics and Astronautics (“NUAA”), a public university located in Nanjing, China. NUAA is operated by the People’s Republic of China’s Ministry of Industry and Information Technology. NUAA is regarded as one of the top engineering universities in China and has significant influence over China’s

aerospace industry. The Ministry of Industry and Information Technology of the Chinese government plays a significant role in regulating major industries and approving new industrial investments and projects in key areas including information technology, telecommunications, and national defense. NUAA is a regular collaborator with Commercial Aircraft Corporation of China (“COMAC”) and Aviation Industries of China (“AVIC”), hosting academic and commercial seminars and symposium and sponsoring researched published by academics from NUAA.

THE VICTIM COMPANIES AND THE PROPRIETARY INFORMATION

8. Victim Company A has offices in the Southern District of Ohio. Victim Company A is among the world’s top aircraft engine suppliers for both commercial and military aircraft. Victim Company A has devoted substantial resources to research and development in the field of using unique materials to manufacture jet engine fan blades and fan containment structures. Worldwide, Victim Company A’s exclusive use of certain types of materials, which provide greater engine durability, weight reduction and lower costs, provides Victim Company A with a significant competitive advantage over its competitors. Victim Company A has spent several decades developing its unique jet engines, engaging in costly trial and error testing in order to advance the use of its products. This testing, research, and development have led to a deep knowledge base that affords Victim Company A a powerful competitive advantage. Release of some or all of this information to a competitor or any other entity attempting to conduct its own research and development in this field would provide a tremendous economic value, because it would enable the other entity to short-circuit its research and development efforts and expend significantly fewer resources.

9. Victim Company A employs several layers of security to preserve and maintain confidentiality and to prevent unauthorized use or disclosure of its trade secrets. These steps were enforced to maintain its competitive advantage and to maintain the integrity of years of research and development pertaining to Victim Company A's use of unique materials to manufacture jet engine fan blades and fan containment structures.

10. Some of the external physical security measures are:

- a. Limiting physical access to restricted portions of Victim Company A's campus; including through the use of manned, gated entrances and requiring identification and access badges; and
- b. Mandating visitor sign-in and escorts.

11. Some of the internal security measures are:

- a. Requiring employee non-disclosure and other confidentiality agreements that extend beyond the length of employment at Victim Company A;
- b. Recurrent training and instruction for employees regarding the processes in place to safeguard restricted and confidential business information;
- c. Notifying all employees that publication and/or disclosure of restricted or confidential company information is prohibited without express company authorization;
- d. Various data security policies; and
- e. Limited access to company proprietary information to employees or contractors on a need-to-know basis.

12. Victim Company B, headquartered in the United States, is one of the world's largest aerospace companies, and a leading manufacturer of commercial jetliners and defense,

space and security systems. Victim Company B provides services, including advanced information and communication systems, and products to both commercial and military aircraft.

13. Victim Company C is a multinational company. Victim Company C produces a variety of commercial products and engineering services. In fact, Victim Company C supplies engines, wheels, brakes, and other aircraft parts to both civilian and military aircraft. Additionally, Victim Company C is a leading U.S. Company in the field of unmanned aerial vehicle (“UAV”) technology.

PROBABLE CAUSE

14. Beginning in at least March 2017, an individual identified as a Deputy Director at NUAA (“Co-Conspirator 1”) began corresponding via email with an individual (“Employee 1”) employed by Victim Company A. Employee 1 has been employed by Victim Company A as an engineer since 2012. With the assistance of XU, Co-Conspirator 1 solicited Employee 1 to come to NUAA for an “exchange” based on Employee 1’s engineering experience at Victim Company A. NUAA offered to pay for Employee 1’s travel expenses.

15. On May 10, 2017, Co-Conspirator 1 emailed Employee 1 that the “Institute of Energy and Power” had proposed that Employee 1 give a report on Victim Company A’s signature materials design and manufacturing technology. Co-conspirator 1 wanted Employee 1 to focus on highly-technical topics, including the latest developments in the application of Victim Company A’s signature material used in aeroengines, as well as engine structure design analysis technology and manufacturing technology development.

16. On May 15, 2017, in preparation for the trip, XU sent a message to Employee 1 from one of XU’s email accounts, but signed the email using the name of Co-Conspirator 1. On

May 25, 2017, Employee 1 traveled to China. Employee 1 gave a presentation at NUAA on June 2, 2017.

17. Following Employee 1's presentation at NUAA, Employee 1 sent messages to Co-Conspirator 1, asking that NUAA delete any and all copies of the presentation from the university computers. The presentation included details regarding engines that were designed and produced by Victim Company A. One of the slides contained the logo of Victim Company A. Employee 1 then emailed a second, edited version of the presentation back to NUAA. The second version deleted the final page of the presentation, as well as content and images from other slides.

18. NUAA reimbursed Employee 1 for expenses incurred during his visit to Nanjing (e.g., meals and hotel expenses). Employee 1 was also paid \$3,500 in U.S. currency for the presentation.

19. While in China, Co-Conspirator 1 introduced Employee 1 to **XU**. During this meeting, **XU** introduced himself using his alias, Qu Hui, and claimed to be from the Jiangsu Science & Technology Promotion Association in China. Employee 1 had meals with **XU** both before and after the NUAA presentation. Employee 1 understood from their conversations that the money paid to Employee 1 came from JAST. **XU** gave a business card to Employee 1 that contains the name Qu Hui and contact information associated with JAST, which, as explained below, are an alias and cover affiliation for **XU**.

20. Employee 1 continued to communicate with **XU** following the trip to China. In fact, **XU** invited Employee 1 to return to NUAA the following year.

21. On November 21, 2017, Co-Conspirator 1 expressed an interest in having Employee 1 “come to exchange and instruct again in NUAA.”¹ Co-Conspirator 1 informed Employee 1 that he had spoken with Qu Hui (XU) from JAST, and that Qu Hui would be able to help with travel expenses and handle the details of the “exchange.”

22. On January 23, 2018, XU, using his alias, sent a message to Employee 1 and informed him that “domestically, there is more focused on the system code.” XU later elaborated that the information he wanted pertained to “system specification, design process.” This term is understood to refer to system code integration -- the application of research data to engine production. XU provided an email address for Employee 1 to use to send the requested information. Employee 1 informed XU that the email may be blocked if he used his company computer. XU responded, “It might be inappropriate to send directly from the company, right?”

23. In response to the “system integration” reference, on February 3, 2018, Employee 1 emailed an excerpt of a presentation from Victim Company A and asked XU if it included the type of information he needed. The attachment was a two-page document from Victim Company A. The first page contained the Victim Company A logo, as well as a Proprietary Label and Warning from Victim Company A. This Warning reads as follows:

Victim Company A Proprietary Information – The information contained in this document is Victim Company A information and is disclosed in confidence. It is the property of Victim Company A and shall not be used, disclosed to others or reproduced without the express written consent of Company A, including, but without limitation, it is not to be used in the creation, manufacture, development, or derivation of any repairs, modifications, spare parts, designs, or configuration changes or to obtain FAA or any other government or regulatory approval to do so. If consent is given for reproduction in whole or in part, this notice and the notice set

¹ Communications in quotation marks are in substance and in part translations from communications that were not originally in English. These translations are subject to revision at a later time.

forth on each page of this document shall appear in any such reproduction in whole or in part. The information contained in this document may also be controlled by the U.S. export control laws. Unauthorized export or re-export is prohibited.”

24. XU also sent Employee 1 a list of technical topics that XU’s organization was interested in. XU wrote, the “attached file is some domestic requirements that I know of, can you take a look and let me know if you are familiar with those?” The attached list stated the following:

Regarding the current development situation and future development direction of foreign countries’ structural materials for fan rotor blades made from composite materials:

[A question followed.]

Regarding the design criteria for the foreign countries’ composite material rotor fan blade, stator fan blade, and fan casing:

[A list of questions followed.]

25. The questions pertain to composite materials in the manufacture of fan blades and fan blade encasements. Victim Company A is the only company in the world that has been producing fan blades and encasements constructed of composite materials. Based upon information provided to me by technical experts at Victim Company A, these questions pertain directly to aspects of Victim Company A’s fan blade and containment system, the materials involved, and Victim Company A’s testing and design systems. For example, according to technical experts at Victim Company A, XU’s questions regarding the “baseline value” and “allowed values” seek proprietary and trade secret information.

26. Employee 1 directly advised XU that some of the posed questions involved Victim Company A’s commercial secrets. XU replied they would discuss it when they met in person.

27. In February 2018, **XU** also began discussing with Employee 1 the possibility of meeting in Europe during one of Employee 1's business trips.

28. **XU** asked Employee 1 to send a copy of the file directory for his company-issued computer. **XU** sent specific directions for how Employee 1 should sort and save such a directory. Following the steps in these directions led to the creation of a document that was essentially a menu of files on the Employee 1's Victim Company A-issued computer. Employee 1 provided a purported file directory to **XU**. This file directory had been heavily edited to remove all sensitive information and was sent with the approval of Victim Company A.

29. On February 28, 2018, at **XU**'s insistence, **XU** and Employee 1 spoke on the phone. During the phone call, **XU** referred to the file directory list Employee 1 sent. **XU** told Employee 1 that "they" had looked at it and it is "pretty good stuff." **XU** asked if Employee 1 would be able to bring it with him when he traveled to Europe for their meeting. **XU** further stated, "the computer you will bring along is the company computer, right?" **XU** also asked if the material Employee 1 intended to bring could be exported out of the computer. Employee 1 informed **XU** that it could be exported onto a portable hard drive. **XU** said, "Good, good, good." **XU** asked, "So, if possible, we will look over the stuff. Can we do that?" Employee 1 agreed to **XU**'s request and **XU** stated, "Do you understand? Carry the stuff along."

30. Later in this conversation, **XU** told Employee 1 that what he was sent so far was "good enough." **XU** continued: "If we need something new later, we can...talk about that in person when we meet. . . What do you think? . . . All right, we really, we really don't need to rush to do everything in one time, because, if we are going to do business together, this won't be the last time, right?"

31. On March 5, 2018, XU sent Employee 1 a message asking, “Regarding the document directory you sent last time, is it possible to dump it to a portable hard drive or USB drive from work computer in advance?”

32. In preparation for the trip to Europe, Employee 1 asked XU where and when he was arriving. XU responded that he would be traveling to Greece before meeting up later with Employee 1 in another country.²

**ADDITIONAL SCHEMES BY XU TO OBTAIN
INFORMATION FROM U.S. AVIATION COMPANIES**

33. Between December of 2013 and December of 2014, XU communicated with an individual, believed to be associated with a university in China, regarding attempts to acquire sensitive information, including analytical tools, design manuals, and software, rightfully belonging to Victim Company B. In these chats, XU discussed plans to travel with another individual to conduct an “exchange” with a “customer.” In late December of 2013, XU and others, believed to be employed by institutions in China, discussed travel arrangements and the types of information that XU’s contact in China was the most interested in obtaining. This information appears to be Victim Company B’s design manual that relates to structural analysis methods. In these exchanges, XU reminded his contact that “[t]he customer doesn’t know our identities. I approached him with the identity of QU Hui, the Deputy Secretary-General of Science and Technology Association.” XU’s associate in China responded, “I will make sure everybody here knows you are from Nanjing Science and Technology Association.”

² Employee 1 has reviewed pictures of XU that were obtained by the FBI. Although Employee 1 did not identify an earlier, younger picture of XU, he did identify XU from a more recent picture.

34. In April 2014, XU communicated with two different individuals believed to be in China. In these messages, XU stated that he was bringing materials related to electric landing gear, deicing, flight control, and electric jet braking. It also appears that some of this material related to a specific type of fueling equipment and/or wing design that pertains to a specific type of military aerial refueling aircraft designed by Victim Company B. XU's articulated plan was to find people in China to read the information, and then review the proposed seminar the recruited "expert" was supposed to give. XU mentioned the possibility of obtaining additional information or "projects" which would include a type of design specification for certain unique technologies, system requirements, and system evaluation, unique to Victim Company B. Once again, XU reminded his contacts of the need to keep his true identity hidden, and stated that he had approached the "expert" using "the name under Jiangsu Science and Technology Association."

35. Various documents obtained in the course of this investigation indicate that XU has contact information pertaining to two individuals believed to be current employees of Victim Company B.

36. In November 2014, XU sent a document to an individual believed to be associated with a Chinese company that engages in the research, development, production, and sale of exhaust turbochargers, engine valves, cooling fans, and other engine parts. The document pertains to a specific technology related to diesel engine variable nozzle turbocharging technology. In communications with the individual, XU explained specific codes contained in the document. For instance, "xxx" meant Ministry of State Security, while "yyy" stood for diesel engine VNT turbocharging technology. There was also a specific code found in this document that referred to Victim Company C.

37. In September 2015, **XU** received emails from an individual employed as an engineer at Victim Company C. This email included an outline of a proposed white paper discussing unmanned aerial vehicle technology. The employee of Victim Company C subsequently sent his resume to **XU**, who forwarded it to NUAA.

LEGAL BACKGROUND

Economic Espionage: 18 U.S.C. § 1831

38. Section 1831 punishes economic espionage for the benefit of any foreign government, foreign instrumentality, or foreign agent:

- (a) Whoever, intending or knowing that the offense will benefit any foreign government, foreign instrumentality, or foreign agent, knowingly --
 - (1) steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains a trade secret;
 - (2) without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys a trade secret;
 - (3) receives, buys, or possesses a trade secret, knowing the same to have been stolen or appropriated, obtained, or converted without authorization;
 - (4) attempts to commit any offense described in any of paragraphs (1) - (3); or
 - (5) conspires with one or more other persons to commit any offense described in any of paragraphs (1) through (3), and one or more of such persons do any act to effect the object of the conspiracy.

Shall, except as provided in subsection (b), be fined not more than \$5,000,000 or imprisoned not more than 15 years, or both.

18 U.S.C. § 1831.

39. The term “foreign instrumentality” means “any agency, bureau, ministry, component, institution, association, or any legal, commercial, or business organization, corporation, firm, or entity that is substantially owned, controlled, sponsored, commanded, managed, or dominated by a foreign government.”

40. The term “foreign agent” means “any officer, employee, proxy, servant, delegate, or representative of a foreign government.”

Theft of Trade Secrets: 18 U.S.C. §1832

41. Section 1832 punishes the commercial theft of trade secrets carried out for economic advantage, whether or not it benefits a foreign government, instrumentality or agent:

(a) Whoever, with intent to convert a trade secret, that is related to a product or service used in or intended for use in interstate or foreign commerce, to the economic benefit of anyone other than the owner thereof, and intending or knowing that the offense will, injure any owner of that trade secret, knowingly—

(1) steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains such information;

(2) without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys such information;

(3) receives, buys, or possesses such information, knowing the same to have been stolen or appropriated, obtained, or converted without authorization;

(4) attempts to commit any offense described in paragraphs (1) through (3); or

(5) conspires with one or more other persons to commit any offense described in paragraphs (1) through (3), and one or more such persons do any act to effect the object of the conspiracy,

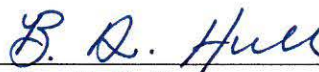
Shall, except as provided in subsection (b) [relating to organizations], be fined under this title or imprisoned not more than 10 years, or both.

18 U.S.C. § 1832(a).

CONCLUSION

42. Based on the foregoing, I believe there is probable cause to find that **XU YANJUN (a/k/a "QU HUI")** has conspired to and attempted to obtain trade secrets from Victim Company A in violation of 18 U.S.C. §§ 1831(a)(4) and (a)(5) (Economic Espionage) and §§ 1832(a)(4) and (a)(5) (Theft of Trade Secrets).

Respectfully submitted,



Bradley D. Hull
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me
on March 21, 2018:


UNITED STATES MAGISTRATE JUDGE